IN THE CLAIMS:

Please amend claim 5 as follows:

1. (Previously Presented) A tamper-resistant modular multiplication method for decreasing the relationship between data processing and consumption current therefor in an information-processing device which includes an input/output port communicating with an external device, a memory device for storing both programs and data, a central processing unit executing the data processing in accordance with said programs, and a bus connecting among the input/output port, the memory device and the central processing unit, when calculating a modular multiplication, A*B*R^(-1) mod N, which appears during performing crypto-processing as the data processing, said method comprising the steps of:

(1) selecting either of the following steps (2) and (3) at random;

(2) calculating S_1 = A*B*R^(-1) mod N where B is a multiplier, A is a multiplicand, N is a product of large primes, and R is 2^ (a bit length of a bit string of data) according to the Montgomery's method of calculating a modular multiplication for the data;

(3) calculating S_2 = {sN + A*(-1)^f}*{tN + B*(-1)^g}R^(-l) mod N, (among arbitrary integers_s, t, f, g, at least one is an integer excepting 0, and f, g are both 0 or 1);

(4) repeating the above-mentioned steps (1), (2), (3) for each bit block consisting of the data, wherein finally when the step (2) is selected for a last bit block of the data, for a calculation result S_1, T_1 = S_1*R^(-1) mod N is calculated to output T_1, and when the step (3) is selected, for a calculation result S_2, T_2 = S_2*R^(-1) mod N is calculated to output N – T_2; and

(5) using T_1 and N - T_2 as a calculation result of a modular multiplication, A*B*R^ (-l) mod N.

2. (Previously Presented) A tamper-resistant modular multiplication method of claim 1, wherein said selecting in the step (1) means to select either one using random numbers.

3. (Original) A tamper-resistant modular multiplication method of claim 1, wherein said (s, t, f, g) are (0, l, 0, 1).

4. (Original) A tamper-resistant modular multiplication method of claim 1, wherein said (s, t, f, g) are (1, 0, 1, 0).

5. (Currently Amended) A tamper-resistant modular multiplication method for decreasing the relationship between data processing and consumption current therefor in an information processing device which includes an input/output port communicating with an external device, a memory device for storing both programs and data, a central processing unit executing the data, processing in accordance with said programs, and a bus connecting among the input/output port, the memory device and the central processing unit, when calculating a modular multiplication, A*B mod p (p is a prime), which appears during performing crypto-processing as the data processing, said method comprising the steps of:

(1) selecting either of the following steps (2) and (3) at random;

(2) calculating S = A*B mod p where B is a multiplier, A is a multiplicand) for a bit string of data;

(3) calculating S = {~~S~~sp + A*(-l)^F~~)~~}*{~~T~~tp + B*(-1)^G} mod p (among arbitrary integers s, t, f, g, at least one is an integer excepting 0, f and g are both 0 or 1, and f + g is an even number); and

(4) using the calculation result S which is selected from said step (2) or (3) as a calculation result of a modular multiplication, A*B mod p.

6. (Original) A tamper-resistant modular multiplication method of claim 5, wherein said (s, t, f, g) are (1, 1, 1, 1).

7. (Previously Presented) A tamper-resistant modular multiplication method of claim 5, wherein the value of f + g in said step (3) is an odd number, and wherein said method further comprising in place of said step (4):

(4) a step wherein when said step (2) is selected the calculation result S is adopted as it is, and when said step (3) is selected, p - S is adopted as a calculation result in place of S; and

(5) a step for adopting said S and p - S as a calculation result of a modular multiplication operation, A*B mod p, for crypto-processing.

8. (Original) A tamper-resistant modular multiplication method of claim 7, wherein said (s, t, f, g) are (0, 1, 0, 1).

9. (Previously Presented) A tamper-resistant modular multiplication method for decreasing the relationship between data processing and consumption current therefor in an information processing device which includes an input/output port communicating with an external device, a memory device for storing-both programs and data, a central processing unit executing the data processing in accordance with said programs, and a bus connecting among the input/output port, the memory device and the central processing unit, when calculating a modular multiplication, $A(x)*B(x) \bmod \Phi(x)$, which appears during performing crypto-processing as the data processing, wherein $\Phi(x)$ is an irreducible polynomial of a variable x and the operation of coefficients of $A(x)*B(x)$ is performed for modulus of a prime p which is 3 or more), said method comprising the steps of:

(1) selecting either of the following steps (2) and 3) at random

(2) calculating $S(x) = A(x)*B(x) \bmod \Phi(x)$, where A(x) or_B(x) is a polynomial of x;

(3) calculating $S(x) = \{s\Phi(x) + A(x)*(-1)\hat{}f\}*\{t\Phi(x) + B(x)*(-1)\hat{}g\} \bmod \Phi(x)$ (among arbitrary integers s, t, f, g, at least one is an integer excepting 0, f and g are both 0 or 1, and f + g is an even number); and

(4) using the calculation result S(x) which is selected from said step (2) and (3) as a calculation result of a modular multiplication, $A(x)*B(x) \bmod \Phi(x)$, for cryptoprocessing.

10. (Original) A tamper-resistant modular multiplication method of claim 9, wherein said (s, t, f, g) are (1, 1, 1, 1).

11. (Previously Presented) A tamper-resistant modular multiplication method of claim 9, wherein the value of f + g in the step (3) is an odd number, and wherein said method further comprises in place of said step (4):

(4) a step wherein when the step (2) is selected the calculation result S(x) is adopted as it is, and when said step (3) is selected, Φ(x) - S(x) is adopted as a result of calculation result in place of S(x); and

(5) a step for adopting said S(x) and Φ(x) - S(x) as a calculation result of a modular multiplication operation, A(x)*B(x) mod Φ(x), for crypto-processing.

12. (Original) A tamper-resistant modulus multiplication method of claim 11, wherein said (s, t, f, g) are (0, 1, 0, 1).

13. (Previously Presented) A tamper-resistant modular multiplication method claim 9, wherein said operation of the coefficients of A(x)*B(x) is performed for modulus of a prime 2 and (f, g) in said step (3) are (0, 0).